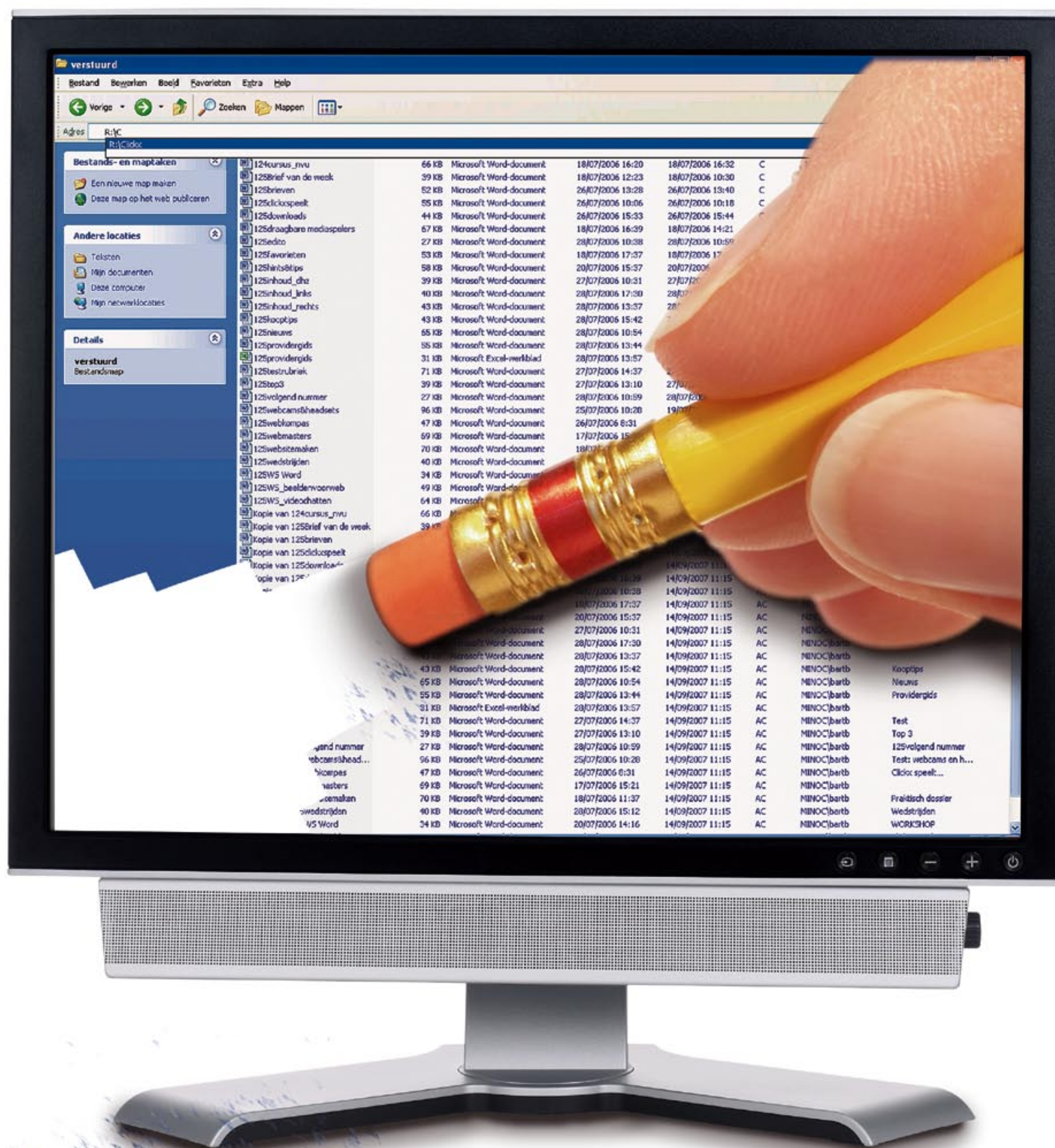
Gegevens definitief verwijderen

Echt gewist?



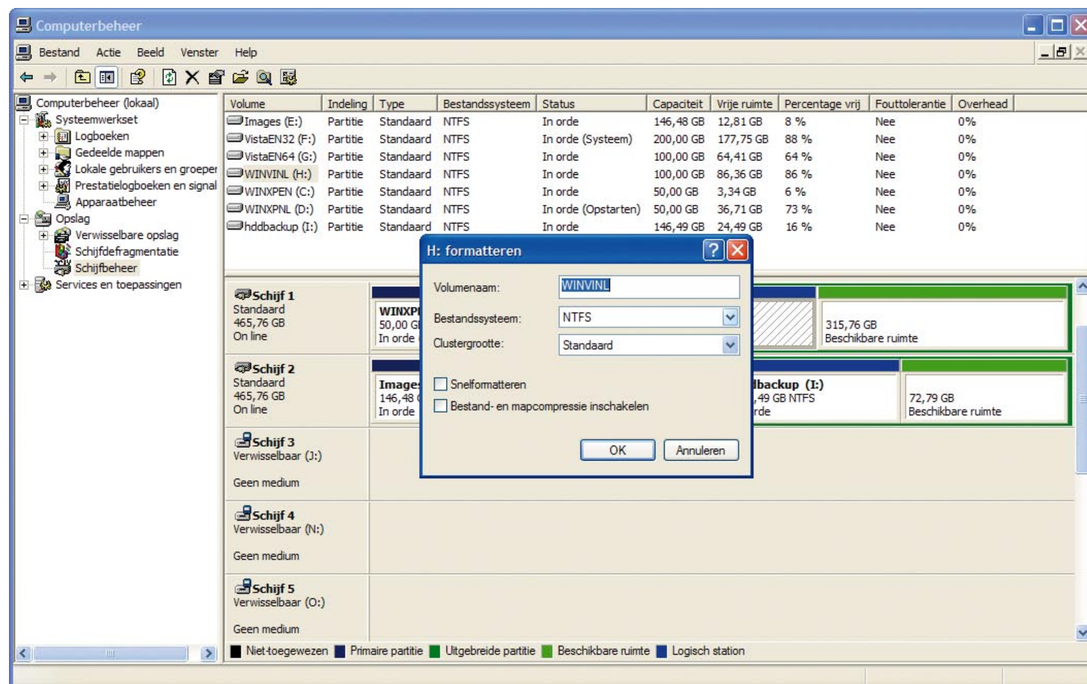
Wil je een oude harde schijf of usb-stick verkopen op eBay? Of gooi je die oude gsm of smartcard weg? Zorg er dan voor dat alle gegevens eerst volledig gewist zijn! Dat lijkt makkelijk, maar in de praktijk is dat helemaal niet zo voor de hand liggend! Hoe ben je zeker dat de gegevens écht verwijderd zijn? FREDERICK GORDTS

Harde schijven worden steeds groter, en wie heeft er geen usb-stick waar gegevens op staan? Ook geheugenkaartjes van digitale camera's bevatten tal van bestanden. Allemaal goed en wel... tot je je harde schijf, usb-stick of geheugenkaart verkoopt. Want dan wil je er toch zeker van zijn dat de koper niet aan jouw persoonlijke gegevens kan. Alle bestanden even wissen in Windows of de schijf formatteren, dat moet toch volstaan, niet? Helaas is het niet zo eenvoudig!

Waar gebeurd



Jan (32) uit Brugge heeft een nieuwe harde schijf gekocht. Met 500 GB zal deze schijf wel enkele jaartjes mee kunnen. Zijn oude schijf – van het merk Maxtor en 100 GB groot – verkoopt hij op eBay voor het luttele bedrag van 14 euro (plus verzendkosten). Toch mooi meegenomen, vindt Jan. Hij formatteert de schijf en stuurt ze op met de post. Netjes geregeld, denkt Jan, tot de koper hem enkele dagen later een persoonlijk document doormailt met de melding "Dit vond ik nog op de schijf!". De koper is gelukkig van goede wil en legt Jan uit dat hij bijna alle bestanden makkelijk terug van de schijf heeft kunnen plukken met een freewareprogramma! Hij belooft om de schijf volledig te wissen en geen misbruik te maken van de bestanden... Dat hoopt Jan althans. Hoe kon de koper die bestanden terugkrijgen, terwijl Jan de schijf toch geformatteerd had? In dit praktisch dossier doen we dit uit de doeken, en laten we je vooral zien hoe je dit vermijdt!



Een partitie formatteren in Windows XP.

Over gegevens en bestanden

Doe je een harde schijf van de hand, dan moet je weten welke gegevens er normaal op zo'n schijf staan. Is dit de enige schijf in je pc, dan kan iemand makkelijk toegang krijgen tot je persoonlijke documenten, maar ook tot je e-mails, favorieten en bankuittreksels, als je die op je computer opslaat. Heb je een bestandje met daarin kredietkaartnummers of toegangscodes voor internetbankieren, dan is ook dit makkelijk te vinden. Of heb je illegaal gekopieerde mp3-bestanden op de schijf staan? Niets weerhoudt de koper ervan dit even door te geven aan de bevoegde instanties... Zelfs al is de verkochte harde schijf niet de primaire schijf in je computer, dan nog staan er waarschijnlijk honderden persoonlijke bestanden op.

En daar houdt het niet bij op: verkoop je een usb-stick, of zelfs een geheugenkaartje voor een digitaal fotoapparaat, dan zijn ook deze bestanden – zelfs gewist of geformatteerd – makkelijk op te sporen. Waarschijnlijk zit je er niet op te wachten dat eender wie je persoonlijke foto's kan zien...

Gewist, of toch niet?

Als je een bestand verwijdert, bijvoorbeeld in Windows, wordt het bestand eigenlijk niet echt verwijderd. Alleen de link naar dat bestand wordt verwijderd (in de zogenaamde Master File Table), zodat het bestand niet meer zichtbaar is in de Verkenner. Het bestand staat echter nog altijd ergens op je harde schijf. Pas als je een nieuw bestand opslaat, of een bestaand bestand opnieuw bewaart, wordt het oude bestand overschreven door het nieuwe. Dat is natuurlijk theorie, want harde schijven zijn tegenwoordig zo groot, dat het dagen of weken kan duren voor de 'resten' van het verwijderde bestand overschreven worden: het valt namelijk niet te voorspellen waar een nieuw bestand wordt weggeschreven – in het begin van de schijf, op het einde, precies daar waar daarnet nog een bestand stond, enzovoort.

Als je een schijf formatteert, gebeurt precies hetzelfde. Alle referenties naar de partities en bestanden worden verwijderd, maar de inhoud van de meeste bestanden blijft gewoon staan. Dat is ook de reden dat formatteren vaak gebeurt in enkele seconden.

Formatteren in Windows XP

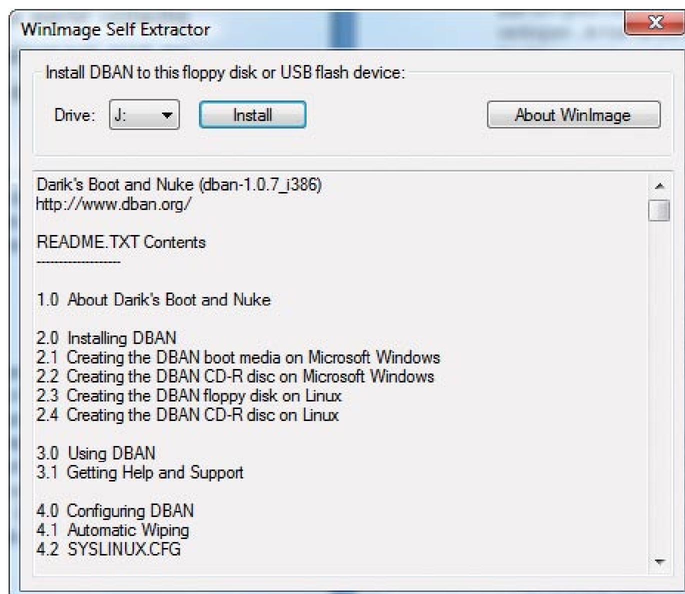
Wil je een schijf formatteren in Windows XP, dan ga je als volgt te werk. Klik met de rechtermuisknop op **Deze computer** en kies **Beheren**. Ga naar **Schijfbeheer**. Je ziet nu netjes elke schijf staan, en alle partities per schijf. Wil je een partitie formatteren, dan klik je er met de rechtermuisknop op en kies je **Formatteren**. We raden je aan om geen vinkje te zetten voor **Snelformatteren**. Je moet alle partities van een schijf formatteren als je die wil verkopen. Je kan de partities ook gewoon wissen, zonder ze te formatteren, door op **Logisch station verwijderen** of op **Partitie verwijderen** te klikken. In beide gevallen zijn er geen bestanden meer zichtbaar op je harde schijf als je die in een computer steekt. Toch kan iemand met de juiste programmaatjes makkelijk je bestanden terughalen. Formatteren of partities verwijderen is dus weliswaar beter dan helemaal niets doen, maar nog lang niet voldoende!

EN ANDERE APPARATEN?

Ook andere apparaten bevatten vaak gevoelige gegevens, zoals gsm's en smartphones. Heeft je gsm of smartphone geen verwijderbare geheugenkaart, dan moet je alle gegevens op de gsm zelf wissen. Dat kan vaak door naar het telefoonboek te gaan en **Alle contacten wissen** te selecteren, of iets in die aard. Vergeet ook niet je sms'jes te verwijderen, en bekijk ook eens de mappen **Verzonden items** en **Concepten**! Heel wat gsm's hebben ook een functie **Fabrieksinstellingen herstellen** of **Restore factory settings** waarmee je alles in één keer kan wissen. Heeft je telefoon wel een geheugenkaart, dan steek je die best in de pc – eventueel met behulp van een adapter – en pas je een van de vermelde methodes (Eraser of UltraShredder) toe.

Veilig wissen

Wil je een harde schijf echt volledig 'veilig' wissen, dan moet je een extra programmaatje gebruiken. Zo'n programma zorgt ervoor dat er over de hele schijf nullen en/of enen komen te staan, zodat alle bestanden effectief gewist worden. De beste programma's doen dit zelfs een aantal keer en telkens op een andere manier. De reden hiervoor is dat harde schijven magnetisch zijn, en er vaak magnetische resten of velden – stukjes bestanden dus – blijven staan, zelfs al worden de gegevens gewist met enen of nullen. Goede programma's gebruiken zelfs beproefde methodes die goedgekeurd zijn door het Amerikaanse ministerie van justitie! Clickx koos drie freewareprogramma's die de klus kunnen klaren.



Dban installeren op een usb-geheugenstick.

1. DBAN

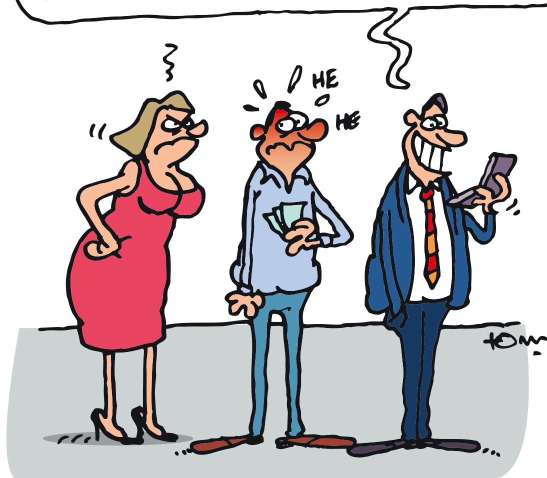
Dban zegt je wellicht niets, maar het is het standaardprogramma om harde schijven veilig te wissen. Dban staat voor Darik's Boot and Nuke, en je vindt het terug op www.dban.org. De webpagina ziet er alvast niet erg gebruiksvriendelijk uit, dus een kleine handleiding is hier zeker op zijn plaats. Dban start je op vanaf een usb-stick, cd-rom of diskette. Op die manier heeft het programma toegang tot alle harde schijven op je pc én kan het dus ook de C-schijf volledig wissen – iets wat onmogelijk is vanuit Windows, omdat die waarschijnlijk ook op diezelfde C-schijf draait.

Wil je Dban installeren op een usb-stick, en dat is het makkelijkste, klik dan op **Download DBAN for installation on floppy disks and USB flash drives**. Vervolgens wordt het bestand – een compacte 1,6 MB – gedownload. Dubbelklik op **dban-1.0.7_i386.exe** en klik op **Uitvoeren**. Selecteer de schijfletter en klik op **Install**. Let wel op: alles wat op je geheugenstick staat, wordt gewist! Heb je geen usb-stick, download dan het bestand voor cd/dvd en brand dit iso-bestand op een cd.

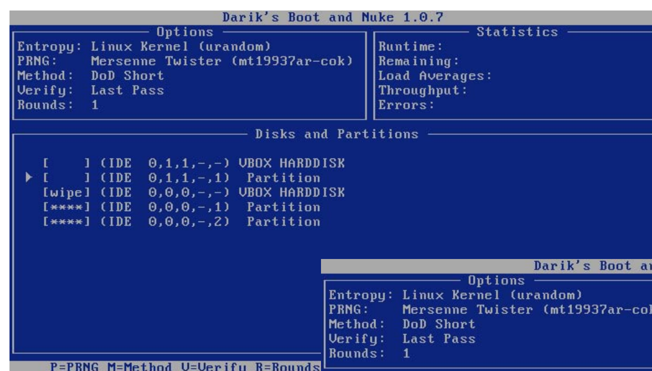
Dban starten gaat als volgt: steek de cd in de cd-lezer of de usb-stick in een usb-poort en start de computer opnieuw op. Druk tijdens het opstarten op **F12** of **F2** of een andere toets – afhankelijk van je computer – om het boot device te kiezen (**Select Boot Device**). Kies nu de usb-schijf of de cd-speler en druk op **Enter**. Vervolgens start Dban op. Druk nogmaals op **Enter** en wacht tot je het blauwe scherm met als titel **Darik's Boot and Nuke** te zien krijgt. Dban is opgestart! De muis werkt niet in Dban, dus moet je alles met het toetsenbord doen. Selecteer eerst de partities die je wil wissen. Heb je maar één harde schijf in je pc zitten, en wil je die wissen, selecteer ze dan allemaal. Partities selecteren doe je door op spatie te drukken, zodat er **WIPE** of **** naast de partitie komt te staan.

Standaard gebruikt Dban de **DoD Short methode** om schijven te wissen. DoD staat voor Department of Defense, of het Ministerie van defensie in de Verenigde Staten. Druk je op de toets **,** (of op **m** op een qwerty-toetsenbord), dan kan je andere methoden selecteren, zoals **DoD 5220.22-M** (nog veiliger) of **PRNG Stream** (nog iets veiliger). Maar hoe veiliger, des te langer het duurt, en de standaardmethode duurt al erg lang. Het wissen van een harde schijf van 250 GB duurt met de standaardmethode bijvoorbeeld al snel 24 uur of langer!

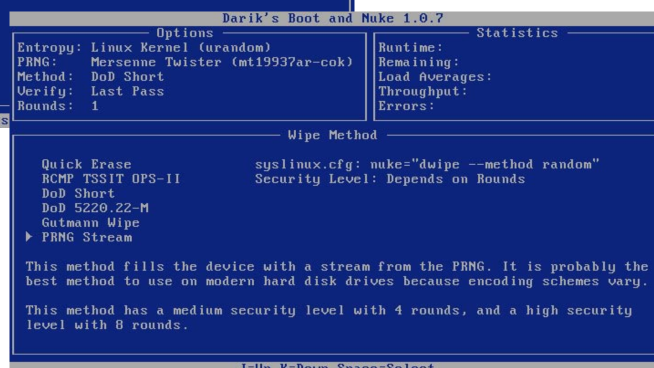
Klaar? Druk dan op **F10** om het wissen te starten. Je kan de voortgang zien op het scherm.



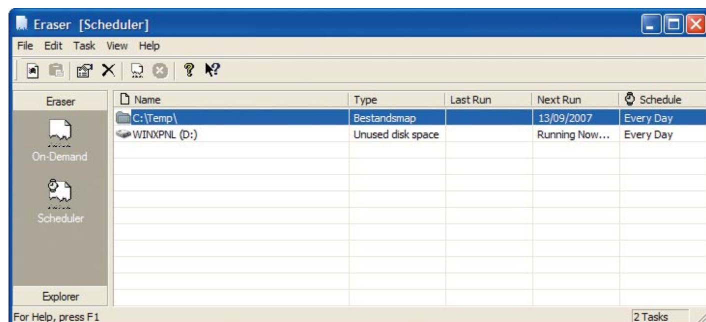
PERSOONLIJKE GEGEVENS UIT JE OUDE GSM VERWIJDEREN



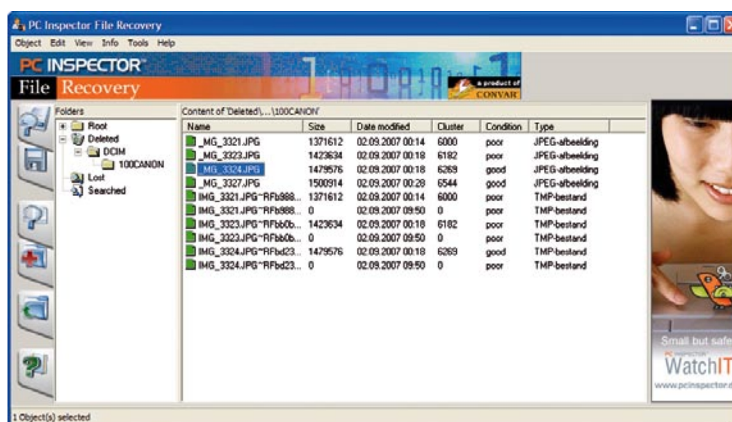
Kies de juiste partitie of harde schijf.



Wissen kan op verschillende manieren.



Eraser is erg gebruiksvriendelijk.



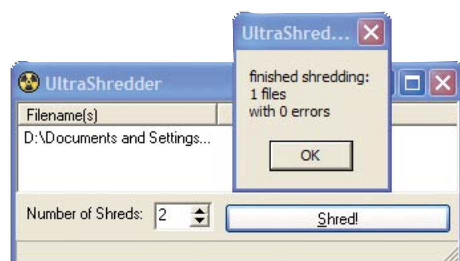
PC Inspector is een stuk gebruiksvriendlijker dan FindNTFS.

2. ERASER

Dban is ideaal om hele partities of harde schijven te wissen, maar lijkt misschien niet zo gebruiksvriendelijk. Hoewel Dban erg kwalitatief 'wist', zijn er nog alternatieven, zoals het gratis Eraser www.heidi.ie/eraser. Dit is een programma dat onder Windows zelf draait. Nadat je het programma geïnstalleerd hebt, kan je het opstarten via **Start, Alle programma's**. Eraser wist geen volledige partities, maar wel lege schijfruimte – ideaal als je net Windows hebt geïnstalleerd maar ervoor wil zorgen dat er op de lege ruimte van de schijf geen bestanden meer teruggevonden kunnen worden. Klik gewoon op **New**, selecteer een schijf en klik op **OK**. Je kan ook zelf bepaalde – gevoelige – bestanden of mappen wissen, maar Eraser kan er ook voor zorgen dat dit automatisch uitgevoerd wordt, bijvoorbeeld elke dag of week op een vastgesteld tijdstip. Klik daarvoor op **Schedule**. Tijdens het wissen kan je je pc gewoon blijven gebruiken.

3. ULTRASHREDDER

Gebruik je vaak andere pc's, bijvoorbeeld op je werk, in een internetcafé of bij een vriend of vriendin? Neem dan UltraShredder www.xtort.net/xtort-software/ultrashredder/ mee. Dit programmaatje – ook gratis – installeer je op een usb-stick. Heb je gedaan met werken op een pc, en wil je er zeker van zijn dat je (tijdelijke) bestanden gewist zijn, steek de usb-stick met UltraShredder dan in de pc en wis je sporen. UltraShredder is erg klein (slechts 300 KB) en kan naar elke usb-stick gekopieerd worden, zelfs als daar al bestanden op staan. Het volstaat om UltraShredder.exe te openen en bestanden naar dit venster te slepen. Klik op **Shred** en je bestanden worden gewist. Let wel op: hoewel de bestanden op een veilige manier gewist worden, is de gebruikte methode minder omvangrijk als bij Dban of Eraser.



Individuele bestanden wissen met UltraShredder.

Zowel met Eraser als met UltraShredder kan je ook probleemloos usb-sticks en geheugenkaartjes voor fotoapparaten wissen. Selecteer gewoon de schijfletter en laat het programma de rest doen.

De proef op de som

Wil je echt weten hoe je bestanden van een harde schijf kan terugvinden? Clickx neemt de proef op de som. We kochten een harde schijf en usb-geheugenstick op eBay en lieten er enkele programmaatjes op los. Een voorbeeld van zo'n programma – dat je trouwens ook zelf kan gebruiken, als je bijvoorbeeld per ongeluk een schijf hebt gewist – is FindNTFS www.partitionsupport.com/utilities.htm. Download de laatste versie, **fntfs205.zip**, en pak het bestand uit in een map. We raden je aan om op dezelfde pagina ook Findpart te downloaden (**fpart487.zip**) en dit bestand in dezelfde map uit te pakken. FindNTFS moet je uitvoeren in DOS. Ga naar **Start, Uitvoeren** en tik **cmd** in, gevolgd door **Enter**. Navigeer nu naar de map waar je FindNTFS hebt geïnstalleerd, bijvoorbeeld **c:\findntfs**. Tik het commando **findntfs 1 1 1 1 log.txt files**. FindNTFS gaat nu op zoek naar verwijderde bestanden op de eerste schijf en de eerste partitie (daarom staat er **1 1 1 1**). Wil je een andere schijf gebruiken, tik dan bijvoorbeeld **2 1 1 1** in.

Eenmaal FindNTFS klaar is, open je het bestand **log.txt** in dezelfde map. Dit bestand bevat alle bestanden die gewist zijn, maar die je nog kan 'recoveren'. Ga op zoek naar een bestand en noteer het nummer van de map van het bestand, bijvoorbeeld **4112**. Vervolgens tik je in: **findntfs 1 1 1 1 copy 4112**. De bestanden in die (verwijderde) map worden nu naar de FindNTFS-map op je pc gekopieerd!

Wij voerden gewoon het commando **findntfs 1 1 1 1 log.txt files** uit en hadden meteen prijs: persoonlijke documenten en afbeeldingen konden we probleemloos bekijken nadat we de op eBay aangekochte harde schijf (€ 40) op onze computer aansloten!

TIP

Partitie vinden

Weet je het nummer van de partitie niet, gebruik dan Findpart om dit te vinden. Tik **findpart all** in en wacht het resultaat af. Vervang de getallen in bovenstaand commando (**findntfs**) door het resultaat van Findpart.

Ook de tweedehands usb-geheugenstick (2 GB - € 15) bevatte nog bestanden. Met het gratis PC Inspector File Recovery www.pcinspector.de/Sites/file_recovery/download.htm?language=46 slaagden we er in een aantal afbeeldingen terug te vinden. De nieuwe versie kan niet alleen bestanden op FAT-partities terugvinden (zoals gebruikt op de meeste geheugenkaarten), maar ook de meer courante NTFS-partities.

Nóg eenvoudiger is Restoration www.snapfiles.com/download/dlrestoration.html, dat – in tegenstelling tot PC Inspector – alle verwijderde bestanden weergeeft in één grote lijst, en dus niet in de originele mappen. Je kan die bestanden dan in één keer terugzetten door op **Restore by Copying** te klikken.

CONCLUSIE

Vooraleer je een harde schijf of usb-stick op eBay verkoopt, zorg je er best voor dat de gegevens volledig gewist zijn, bijvoorbeeld met Eraser, UltraShredder of Dban. Je kan trouwens zelf testen of dit gelukt is, met tools als FindNTFS of – nog eenvoudiger – PC Inspector of Restoration. Ga er niet van uit dat jouw harde schijf 'toch geen data meer bevat'; bij al onze tests vonden wij steevast gewiste bestanden terug! ♦